Cloudflare Bot Management

CAPTCHA 없이 악성 봇을 차단하고 AI 봇을 관리하세요.

트래픽 속에 숨어 있는 봇. 수익과 UX를 해치는 악성 봇.

인터넷 애플리케이션 트래픽의 **30%**는 자동화된 트래픽입니다[1]. 지리적 위치 및 IP 기반 휴리스틱과 CAPTCHA 인증과 같은 기존 방어 방식은 최신 봇에 의해 쉽게 우회됩니다. 이는 실제 사용자에게 큰 불만을 야기합니다.

Cloudflare는 웹의 **약 20%**를 파악하고 있으므로 Cloudflare보다 더 많은 AI 크롤러와 검색 봇을 식별하는 곳은 없습니다[2].

Cloudflare Bot Management는 조직들이 CAPTCHA 없이 웹 및 모바일 애플리케이션으로 향하는 AI 크롤러와 봇 트래픽을 관리하는 데 도움이 됩니다. 검증된 봇 및 규제 준수 AI 크롤러를 애플리케이션에 허용하고, 규제를 준수하지 않는 AI 봇과 악성 봇을 식별하여 차단합니다. 이는 Cloudflare의 애플리케이션 보안 포트폴리오의 핵심 기능입니다.

제품의 이점

- 사기, 금전적 손실 및 브랜드 이미지 손상 방지
- 더 나은 웹 및 모바일 애플리케이션 경험 제공
- 원치 않는 AI 크롤러 및 검색 봇으로부터 해방

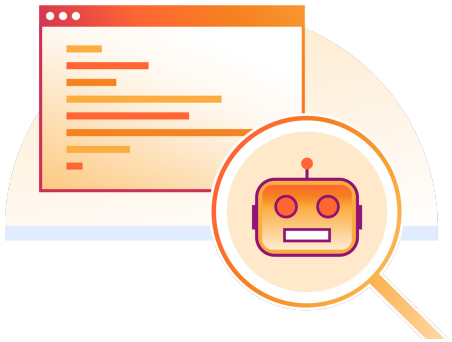

그림 1: 애플리케이션 보안 포트폴리오에 통합된 Cloudflare Bot Management

출처

1. Cloudflare Radar 데이터, 2024년
2. W3techs, 리버스 프록시 서비스의 사용량 통계 및 시장 점유율, 2025년

Cloudflare Bot Management의 작동 방식

Cloudflare는 전 세계 및 애플리케이션별 머신러닝, 클라이언트 측 JavaScript, 모바일 기기, 그리고 휴리스틱 기반의 다층 감지 시스템을 결합하여, 모든 HTTP 요청마다 단일한 봇 점수를 부여합니다. 봇 점수는 해당 요청이 봇에서 왔을 가능성이 얼마나 되는지를 나타냅니다. 이 봇 점수는 차단 또는 허용과 같은 표준 응답과 다른 Cloudflare 제품을 통한 사용자 지정 응답 정책에 사용됩니다. 봇 점수, HTTP 요청 메타데이터 등을 포함한 봇 분석은 Cloudflare 대시보드 UI 또는 타사 도구에서 Cloudflare API를 통해 사용할 수 있습니다.

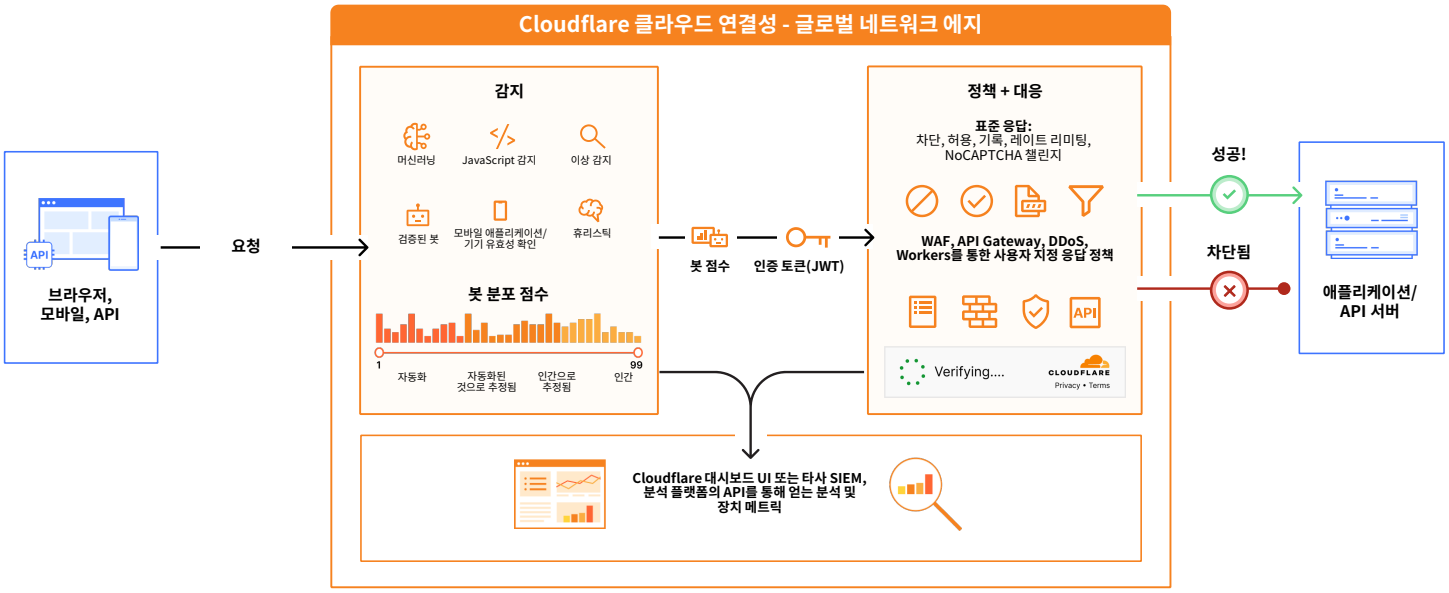

그림 2: Cloudflare Bot Management를 거치는 샘플 요청 경로

Cloudflare Bot Management 주요 기능

계정 탈취 및 악용 방지

공개하는 것보다 빠르게 취약점을 감지할 수 있는 ML 지원 모델로 zero-day 공격을 방어합니다. 기록적인 DDoS 공격을 방어하고, 중요한 데이터를 보호하며, 클라이언트 측 위험을 줄이고, 웹 애플리케이션의 소프트웨어 공급망을 모니터링합니다.

봇 및 사기로부터 방어

계정 탈취로부터 사용자를 보호하고 최종 사용자 경험에 영향을 미치는 악성 봇을 차단합니다. ML 모델을 클라이언트, 네트워크, 위협 인텔리전스와 결합하여 악의적인 봇넷, 자격 증명 및 카드 스터핑, 콘텐츠 스크래핑, 재고 사재기를 차단합니다.

AI 크롤러 및 봇 관리

AI 크롤러를 차단하고, 요금을 부과하거나, 무한 루프에 가두어 콘텐츠 및 비용에 대한 통제력을 강화하세요. 요청 패턴에 대한 가시성을 확보하고 robots.txt 지침 준수 여부를 확인하세요. 모든 Cloudflare 고객이 사용할 수 있습니다.

주요 기능	
감지 엔진	
머신러닝	매일 수십억 건의 요청을 프록시하는 Cloudflare의 전역 네트워크 트래픽 전체를 대상으로 Cloudflare의 글로벌 머신러닝 모델을 학습시켜 자동화된 트래픽과 인간에 의한 트래픽을 식별합니다. 이 결과는 전체 봇 점수에 포함됩니다. 고객은 최신 모델로 자동 업데이트됩니다.
이상 감지	Cloudflare의 비지도 학습 행동 이상 탐지 모델은 애플리케이션별 트래픽 패턴을 기준으로 삼고, 고객의 트래픽 패턴이 시간에 따라 변화함에 따라 규칙 임계값을 조정하여 비정상적인 봇 활동을 식별합니다. 이 결과는 전체 봇 점수에 포함됩니다.
휴리스틱	이전 봇 트래픽에서 나타난 악성 봇의 알려진 행위 패턴을 이용하여 봇을 식별합니다. Cloudflare는 모든 고객을 위해 휴리스틱을 정기적으로 업데이트하고 있습니다. 이 결과는 전체 봇 점수에 포함됩니다.
검증된 봇 및 AI 봇	Cloudflare의 봇 디렉터리는 Cloudflare 검증된 봇 정책에 따라 검증된 봇으로서 합법적인 기능을 수행하고 투명하게 작동하는 알려진 봇 감지 ID를 식별합니다. 알려진 AI 봇에 대해서는 별도의 카테고리가 있으며, 이 봇은 robots.txt를 준수할 수도, 그렇지 않을 수도 있고, 애플리케이션에서 동작을 숨길 수도 있습니다.
JavaScript 감지	JavaScript 감지 모듈이 요청의 클라이언트 측에서 가볍고 보이지 않는 JavaScript를 삽입하여 헤드리스 브라우저 및 기타 악의적 지문을 식별합니다. Cloudflare는 매우 엄격한 개인 정보 보호 표준을 준수하며 이 과정에서 개인 식별 정보를 수집하지 않습니다.
봇 점수	각 봇 ID 또는 유형에 대한 규칙을 작성하는 대신 봇 점수를 사용하여 더 적은 수의 규칙으로 대부분의 봇을 포착합니다. 봇 점수는 Cloudflare 감지 엔진의 인텔리전스를 결합하여 1부터 99까지의 점수를 만들어, 해당 요청이 봇에서 발생한 가능성이 얼마나 되는지 나타냅니다. 점수 1점은 확실히 자동화된 요청을 의미하며, 99점은 확실히 사람이 보낸 요청을 의미합니다.
모바일 장치 SDK를 이용한 장치 유효성 확인	Android, iOS, React Native, Unity 등을 포함한 모든 주요 모바일 애플리케이션 플랫폼용 SDK는 애플리케이션 무결성을 검증하고, 안전하지 않은 환경을 탐지하며, API 트래픽을 인증합니다(자체 제공 또는 Cloudflare 승인 암호화 토큰 사용).
정책 및 대응	
표준 응답	Cloudflare 감지 엔진에서 식별한 봇 트래픽에 대한 응답으로 차단, 허용, 기록, 레이트 리미팅 또는 다양한 사용자 친화적인 챌린지를 설정합니다.
사용자 지정 응답 정책	Cloudflare WAF, DDoS와 같은 다른 Cloudflare 제품의 정책에 봇 관리 신호를 통합하고 Workers를 통해 사용자 지정 작업을 작성합니다.
분석	
Cloudflare 대시보드	최대 30일 전의 봇 활동을 검토하고 봇 점수와 기타 봇, 트래픽 및 요청 필터를 기준으로 필터링합니다. 봇 피드백 루프를 통해 고객은 Cloudflare에 긍정 오류 또는 부정 오류를 보고하여 추가 조사를 요청할 수도 있습니다.
타사 도구(SIEM, 데이터 레이크, 분석 도구 등)	Cloudflare Security Analytics를 통해 하나의 대시보드에서 모든 애플리케이션의 Bot Management 신호를 분석하고, Log Explorer에서 추가 로그 데이터를 탐색하고, Log Push를 통해 타사 SIEM 또는 분석 플랫폼에서 타사 데이터와 Cloudflare 데이터를 결합합니다.

자세히 알아보고 싶으신가요? 애플리케이션 보안 데모 시리즈에 등록하세요.